Remarks

Claims 1-25 and 27-37 are pending in the application. All claims stand rejected by the Office Action dated November 15, 2006. By this paper, claims 1, 7, 12, 15 and 21 have been amended, claims 11 and 35 have been canceled without prejudice or disclaimer, and claims 38-46 have been added. The amendments have not introduced new matter. Support is found for the amendments of claims 1, 15 and 21, and for the new claims 38-46 in paragraphs [0011], [0037], [0038], [0059], and [0060], for example.

Preliminary Matters

Claim 7 has been amended herein to correct an error made in Applicants' Amendment filed October 13, 2005 in which the language of claim 6 was mistakenly used in place of claim 7 without an indication that claim 7 had been amended. The amendment to claim 7 shown in the listing of claims above adds the word "an" and otherwise restores claim 7 to its original state.

Also, Applicants note that the last 3 lines of page 18 and the first 3 lines of page 19 of the original specification state "attempt to log into the first network device 110 using a series of protocols (e.g., Windows Networking Protocol (developed by Microsoft of Redmond, WA), Secure Shell (SSH) ***(developed by SSH Communications Security Ltd. of Palo Alto, CA), telnet, ftp, etc.). Once*** logged in, the scanning module 135 can query the first network device 110 for data, such as by looking for the presence of the file /etc/passwd to deduce a UNIX computer, or perform a Registry query on a Windows computer." The highlighted text has been omitted from paragraph [0058] of the publication of the present application (U.S.

Patent Application Publication No. 2005/0097199). Applicants request appropriate correction to the published application and any patent issuing from the present application.

Claim Objection

Claim 35 was objected to as being a substantial duplicate of claim 34. Applicants have canceled claim 35 herein without prejudice or disclaimer, mooting this objection.

35 U.S.C. § 112, First Paragraph

Claims 1, 15 and 21 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to provide enablement for "performing remote agentless scanning of internal files and data within the internal files." Applicants respectfully traverse this rejection.

FIG. 4 of the present application provides an example embodiment for remote agentless scanning of internal files and data within the internal files on a first network device. As shown in FIG. 4, remote agentless scanning includes determining properties (step 445), determining an identity of a network device (step 450), determining what to scan (step 455), and performing the scan (step 460). As discussed below, the example shown in FIG. 4 and the corresponding discussion in the specification clearly enable a person of ordinary skill in the art to make and use the apparatus and methods in claims 1, 15 and 21.

In particular, the specification clearly teaches that performing remote agentless scanning of internal files and data within the internal files on the first network device may be accomplished by, for example, gaining access to the internal files by logging onto the first network device. See, paragraph [0011]. Thus, as part of the scanning process, in one embodiment, login information is determined. See, paragraph [0057] (indicating that "a user name and password to log into the first network device 110" are among the properties determined in step 445 of FIG. 4).

Once logged in, the specification clearly enables remote agentless scanning of ***internal files*** by, for example, searching for specific files on the first network device 110. "For example, on a Microsoft Windows computer 110, the scanning module 135 may scan for missing Windows Hotfixes. On a Solaris® computer...the scanning module 135 can scan for missing Solaris® patches." Paragraph [0059].

The specification also clearly enables remote agentless scanning of ***data within internal files*** on the first network device 110. See, paragraph [0011] ("logging into the first network device and/or querying data within the device"). This may be done, for example, by performing a Registry query on a Windows computer as disclosed in paragraph [0058]. (As discussed above, the published application confuses this aspect of paragraph [0058] in the original specification, which states that "[o]nce logged in, the scanning module 135 can query the first network device 110 for data, such as by looking for the presence of the file /etc/passwd to deduce a UNIX computer, or perform a Registry query on a Windows computer.")

An artisan would recognize that the Windows Registry in a Microsoft Windows operating system stores information and settings for hardware, operating system

software, most non-operating system software, users, preferences, etc. Thus, data within the first network device 110 may be scanned to determine, for example, "policy settings" (see paragraph [0059]), security settings (see paragraph [0060]), and/or other data stored internally on the first network device 110.

Applicants respectfully submit that the level of detail provided in the application, particularly in FIG. 4 and paragraphs [0057]-[0062], clearly enable a person skilled in the art to make and use the claimed invention. See M.P.E.P. § 2164.01 (stating that a "patent need not teach, and preferably omits, what is well known in the art"). Thus, Applicants respectfully request that the rejection under 35 U.S.C. § 112, first paragraph, be withdrawn.

35 U.S.C. § 103(a)

Claims 1-4, 6-12, 14-18, 20-24, 27-31 and 33-36 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Application Publication No. 2003/0212779 by Boyter et al. ("Boyter") in view of U.S. Patent No. 6,993,448 to Tracy et al. ("Tracy"); claims 13, 19 and 25 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Boyter in view of U.S. Patent Application Publication No. 2004/0268145 by Watkins et al. ("Watkins"); claim 5 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Boyter in view of U.S. Patent Application Publication No. 2001/0047401 by Moore et al. ("Moore"); and claims 32 and 37 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Boyter in view of U.S. Patent No. 6,546,493 to Magdych et al. ("Magdych").

As discussed below, Applicants respectfully traverse these rejections because the cited references, alone or in combination, fail to teach or suggest the elements of the claims. See M.P.E.P. § 2143 (stating that in order to establish a *prima facie* case of obviousness for a claim, the prior art references must teach or suggest all the claim limitations).

The cited references do not teach or suggest remote agentless scanning of internal files and data to determine internal security settings.

Claims 1, 15 and 21 are amended herein to recite, among other things, "***remote agentless scanning of internal files and data*** within the internal files on the first network device ***to determine internal security settings*** therefrom." (Emphasis added). Applicants respectfully submit that the cited references, either individually or when combined, do not teach this limitation.

According to page 4 of the Office Action, "Boyter et al fails to teach performing remote agentless scanning of internal files and data within the internal files." Thus, Boyter cannot perform such remote agentless scanning of internal files and data to determine internal security settings.

Page 4 of the Office Action also cites Tracy for teaching a network scanner that can obtain an IP address, a host name, a MAC address, an operating system (OS) and an OS version. Page 4 of the Office Action further asserts that Tracy teaches a "host profiler that can determine information about the hardware configuration, operating system option, installed software, etc." See also, col. 8, lines 36-41 (indicating that the information collected by the host profiler includes IP address, MAC, Hostname, OS, Version, mfr, model, CPU, CPU Qty, CPU Speed,

RAM, Disk Space, and Software). However, Applicants respectfully assert that such information is not "internal security settings."

By way of contrast with Tracy, the independent claims of the present application, as amended herein, determine internal security settings through a remote agentless scan of internal files and data. For example, as disclosed in paragraph [0037] of the present application, "the scanning module 135 can scan the first network device 110 for the latest patches, to determine if anti-virus software is installed, to determine whether firewall software is installed (and what kind)...." See also, paragraph [0059] (internally scanning for missing Windows Hot-fixes and/or missing Solaris patches). Applicants submit that Tracy is silent as to determining such internal security settings through a remote agentless scan of internal files and data.

Further, Applicants respectfully submit that Tracy is silent as to whether any data is collected through remote agentless scanning of internal files and data. Nowhere does Tracy indicate that agents are not used. Rather, Tracy provides several examples of the network discovery engine 606 (which includes the network scanner 702 and the host profiler 704) using external (port) or agent data collection. See, for example, col. 6, lines 60-63 (TCP/UDP ***port interrogation***); and col. 6, line 64 and col. 7, lines 16-19 (indicating that SNMP can be used to acquire additional information such as device manufacturer, model, and application software ***if a queried network device 614a-n is SNMP enabled***).

Regarding the host profiler 704 (again, which is part of the network discovery engine 606), col. 7, lines 50-51 of Tracy indicates that the "host profile can be

conventional enterprise management software." However, Tracy previously indicates in col. 7, lines 19-25 that enterprise management software can only be used "if a network device 614a-n utilizes (e.g., has installed thereon) an Enterprise Management (EM) software/system." Thus, Tracy clearly teaches using agents (e.g., an SNMP agent or enterprise management agent) stored on the network devices.

The cited references do not teach or suggest automatically installing security software based on an evaluation of internal security settings.

Claims 1 and 15 are amended herein to recite, among other things, "(c) comparing the internal security settings determined through the remote agentless scanning with predefined security settings to determine compliance therewith; and (d) ***automatically performing a remote installation of a security software program*** on the first network device ***if the internal security settings are not in compliance*** with the predefined network settings." (Emphasis added).

Applicants respectfully submit that the cited references, either individually or when combined, are silent as to installing security software based on an evaluation of internal security settings. By way of contrast with the cited references, paragraphs [0037] and [0038] of the present application disclose scanning for latest patches, anti-virus software, and/or firewall software and fixing deviations is security policy by automatically applying patches. See also, for example, paragraph [0011] (installing automatically installing anti-virus software); and paragraph [0060] (comparing scanned security settings to pre-defined security settings).

Conclusion

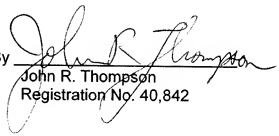
As the cited references do not disclose all of the claimed limitations, Applicants respectfully request that the rejection of independent claims 1, 15 and 21

be withdrawn. As the depending claims include the limitations of the independent claims, they likewise represent patentable subject matter.

Should there remain any issues that may be resolved by a telephone conference, the Examiner is invited to contact the applicant's representative below. Reconsideration of all pending claims in view of the amendments and remarks is respectfully requested.

Respectfully submitted,

Altiris, Inc.

By 
John R. Thompson
Registration No. 40,842

STOEL RIVES LLP
One Utah Center Suite 1100
201 S Main Street
Salt Lake City, UT 84111-4904
Telephone: (801) 328-3131
Facsimile: (801) 578-6999